Главное следственное управление СКР по Красноярскому краю предлагает Вашему вниманию рекомендации по мерам безопасности в сети Интернет

Рекомендации о мерах безопасности в сети Интернет (вредоносное ПО, кража паролей)

1. Обязательно установить антивирусную программу и периодически ее обновлять.

2. Установить и включить брандмауэр.

3. На домашнем беспроводном Wi-Fi-устройстве (маршрутизатор) установить защиту паролем.

4. Перед переходом по ссылкам или открытии вложений, пришедших по электронной почте, убедиться, что Вам известен отправитель.

5. Не переходите по подозрительным ссылкам и не нажимайте на кнопки всплывающих

подсказок, которые также выглядят подозрительно.

6. Никогда не сообщайте свои персональные сведения (такие как номер счета или пароль) если их запрашивает по электронной почте неизвестный Вам адресат, а также, если они запрашиваются в социальной сети.

7. Обязательно настройте ваши аккаунты социальных сетей так, чтобы Ваш профиль могли просматривать только пользователи, которые допущены к просмотру вашего профиля.

8. Контролируйте добавленные комментарии о Вас.

9. Научитесь блокировать пользователей пишущих нежелательные комментарии о Вас.

10. Ни в коем случае не публикуйте информацию, которую Вы не хотели бы видеть на доске объявлений.

11. Подходите очень избирательно к предложениям дружбы.

12. Постоянно анализируйте, кто из пользователей имеет доступ к Вашим страницам, а также периодически просматривайте информацию, которую эти пользователи публикуют о Вас.

13. Проведите с детьми инструктаж и постоянно контролируйте их действия в Интернете.

14. Обязательно обращайте внимание на то, чем дети занимаются в Интернете и с кем они там общаются.

15. Создавайте резервные копии важных документов на автономных носителях.

Рекомендации о мерах безопасности в сети Интернет (мошенничество)

Покупки через Интернет – это без сомнения очень удобно. Сфера Интернет-услуг расширяется, доходы сетевых ритейлеров растут, а люди все чаще предпочитают заказ товаров в сети походам по магазинам.

Мошеннический интернет-магазин можно идентифицировать по нескольким признакам. Если Интернет-магазин или объявление соответствуют хотя бы одному из указанных ниже признаков, это серьезный повод задуматься о целесообразности совершения сделки. Если под их описание подходят два или более признака, мы настоятельно рекомендуем Вам воздержаться от контактов с данным продавцом или магазином.

1. Низкая цена. Если вы нашли объявление или магазин, предлагающий товары по ценам, существенно ниже рыночных, имейте в виду, что мошенники часто используют данный прием

для привлечения жертв. На что следует обратить внимание? Посмотрите стоимость аналогичных товаров в других Интернет-магазинах, она не должна отличаться слишком сильно. Не поддавайтесь на слова «акция», «количество ограничено», «спешите купить», «реализация таможенного конфиската», «голландский аукцион».

2. Требование предоплаты. Если продавец предлагает перечислить предоплату за товар, особенно с использованием анонимных платежных систем, электронных денег или при помощи банковского перевода на карту, выданную на имя частного лица, нужно понимать, что данная сделка является опасной. На что следует обратить внимание? Учитывайте риски при совершении Интернет-покупок. Помните о том, что при переводе денег в счет предоплаты вы не имеете никаких гарантий их возврата или получения товара. Если вы решили совершить покупку по предоплате, проверьте рейтинги продавца в платежных системах.

3. Отсутствие возможности курьерской доставки и самовывоза товара. Данные факторы вынуждают покупателей пользоваться для доставки товара услугами транспортных компаний и, соответственно, вносить предоплату. На что следует обратить внимание? Выбирая из нескольких магазинов, следует отдать предпочтение тому, в котором есть возможность забрать товар самостоятельно. Злоумышленники могут предоставить поддельные квитанции об отправке товара транспортной компанией.

4. Отсутствие контактной информации и сведений о продавце. Если на сайте Интернет-магазина отсутствуют сведения об организации или индивидуальном предпринимателе, а контактные сведения представлены лишь формой обратной связи и мобильным телефоном, такой магазин может представлять опасность. Очень часто злоумышленники указывают несуществующие адреса, либо по данным адресам располагаются совсем другие организации. Проверьте отзывы о магазине в открытых Интернет-рейтингах, пролистайте отзывы как можно дальше, злоумышленники могут прятать негативные отзывы за десятками фальшивых положительных оценок. В случае совершения покупок посредством электронных досок объявлений посмотрите историю сделок продавца и ознакомьтесь с его рейтингом, многие торговые площадки предлагают подобную услугу.

5. Отсутствие у продавца или магазина «истории». Если Интернет-магазин или учетная запись продавца зарегистрированы несколько дней назад, сделка с ними может быть опасной. Создание Интернет-магазина – дело нескольких часов, изменение его названия и переезд на другой адрес – дело нескольких минут. Будьте осторожны при совершении покупок в только что открывшихся Интернет-магазинах.

6. Неточности или несоответствия в описании товаров. Если в описании товара присутствуют явные несоответствия, следует осторожно отнестись к подобному объявлению. Внимательно прочитайте описание товара и сравните его с описаниями на других Интернет-ресурсах.

7. Излишняя настойчивость продавцов и менеджеров. Если в процессе совершения покупки

менеджер магазина начинает торопить Вас с заказом и оплатой товара, убеждая в том, что если не заказать его сейчас, то цена изменится или товар будет снят с продажи, не поддавайтесь на уговоры и трезво оценивайте свои действия. При наличии любых сомнений откладывайте сделку.

8. Подтверждение личности продавца путем направления отсканированного изображения паспорта. Ожидая перевода денег, продавцы в социальных сетях часто направляют изображение своего паспорта покупателю с целью подкупить его доверие. Помните, что при современном развитии техники изготовить изображение паспорта на компьютере не представляет никакого труда. Данное изображение никаким образом не может подтверждать личность лица, направившего его вам.

9. Не отвечайте на любые просьбы прислать деньги от «членов семьи» или «друзей», «родственников», на сомнительные предложения о сделке, на всевозможные сообщения о лотерейных розыгрышах, в которых вы не принимали участия.

20 Сентября 2017

Адрес страницы: https://krk.sledcom.ru/news/item/1165593